

# Oracle Integrated Lights Out Manager

Security Configuration Supplement for the  
United States Department of Defense

ORACLE WHITE PAPER | AUGUST 2016





## Table of Contents

Overview	4
Product Description	4
Product Security Guide	4
Version and Update Information	5
Security Configuration Information	5
Default Accounts and Passwords	5
Default Exposed Network Services	7
Security Configuration Hardening	8
Enable FIPS 140 Compliant Operation	8
Disable Unnecessary Services	8
Check that HTTP Redirection to HTTPS is Enabled	10
Check that SSLv2 Protocol for HTTPS is Disabled	10
Check that SSLv3 Protocol for HTTPS is Disabled	10
Check that Unapproved TLS Protocols for HTTPS are Disabled	11
Check that SSL/TLS Weak and Medium Strength Ciphers for HTTPS are Disabled	11
Check that Unapproved SNMP Protocols are Disabled	12
Configure SNMP Community Strings	12
Replace Default Self-Signed Certificates	13
Configure Administrative Interface Inactivity Timeout (Browser)	13
Configure Administrative Interface Inactivity Timeout (CLI)	14
Configure Login Warning Banners	14
Management Network Recommendations	15



## Overview

United States Department of Defense (DoD) Instruction 8500.01 (effective March 2014) instructs DoD Component Heads to "ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs with any exceptions documented and approved by the responsible authorizing official (AO)." Within the DoD, Security Technical Implementation Guides (STIGs) help to define the security configuration baselines for IA and IA-enabled devices. Specifically, STIGs contain prescriptive steps that can be used to both assess and improve the security configuration of systems and devices deployed on DoD networks. For more information on DoD STIGs, see: <http://iase.disa.mil/stigs/Pages/index.aspx>.

As of this white paper's publication, STIGs can only be developed when they align to one of the published DoD Security Requirements Guides (SRGs) per the STIG development vendor process, documented at: <http://iase.disa.mil/stigs/Pages/vendor-process.aspx>. Unfortunately, while the published SRGs map to common technology areas, there is no suitable SRG for IT appliances. As a result, it is not possible to publish a STIG for the Oracle Integrated Lights Out Manager (ILOM) as it is a dedicated, fixed-function appliance.

To mitigate this shortcoming, this technical white paper will provide prescriptive security configuration hardening guidance that will allow DoD customers to improve upon the default security configuration of Oracle ILOM in a manner suitable to what would otherwise have been published as a DoD STIG.

## Product Description

The Oracle ILOM provides advanced service processor hardware and software that can be used to manage and monitor Oracle Sun servers. Oracle ILOM's dedicated hardware and software is pre-installed on Oracle's Sun server platforms including SPARC and x86-based servers as well as on Oracle appliances such as Oracle Exadata Storage Servers, Oracle ZFS Storage Appliance, as well as a variety of Oracle InfiniBand and Ethernet switches. The Oracle ILOM enables customers to actively manage and monitor the underlying server or device independently of the operating system state, providing a reliable lights out management capability. With Oracle ILOM, customers can:

- » Learn about hardware errors and faults as they occur
- » Remotely control the power state of the server platform
- » Access the console of the server platform using graphical and non-graphical means
- » Determine the hardware inventory and configuration of the system
- » Receive generated alerts about system events
- » Monitor environmental and power conditions

## Product Security Guide

This white paper is intended to provide common information and procedures necessary to validate and further improve the "out of the box" security configuration of this product. The Oracle Integrated Lights Out Manager Security Guide, available as a standard part of the Oracle product documentation, has additional information on the product's security features, capabilities and configuration options. It is strongly recommended that customers review the product security guide before implementing the recommendations contained within this technical white paper.

- » Oracle Integrated Lights Out Manager (ILOM) Security Guide for Firmware 3.0, 3.1 and 3.2  
[http://docs.oracle.com/cd/E37444\\_01/pdf/E37451.pdf](http://docs.oracle.com/cd/E37444_01/pdf/E37451.pdf)

---

*Always review the correct version of the product security guide as the security features, capabilities and configuration options will often vary based upon product version.*

---

## Version and Update Information

To leverage the most recent features, capabilities and security enhancements, customers are encouraged to update their Oracle ILOM software to the latest, supported version for their respective hardware platform. To determine the version of the Oracle ILOM software that is being used on the platform, execute the following command after first logging into the Oracle ILOM.

```
-> version
SP firmware 3.2.6.26.a
SP firmware build number: 109322
SP firmware date: Wed Apr 6 14:31:00 CST 2016
SP filesystem version: 0.2.10
```

In the above example, the Oracle ILOM software is version 3.2.6.26.a. For detailed instructions describing how to update the Oracle ILOM software, refer to the "Performing Firmware Updates" section of the Oracle Integrated Lights Out Manager Configuration and Maintenance Guide.

As a convenience the latest version of ILOM available for each type of Oracle Server or Switch is listed on the Oracle Technology Network (OTN) Firmware page:

<http://www.oracle.com/technetwork/systems/patches/firmware/release-history-jsp-138416.html>

As of the date of this document the latest ILOM version is 3.2.6 which is available for many recent servers. To download a release, go to My Oracle Support at <https://support.oracle.com/>. Note that the latest ILOM version listed should only be installed on servers and switches that are not a part of an Oracle Engineered System or Appliance. The ILOMs for Engineered Systems and Appliances should only be updated as a part of an update provided by Oracle for that Engineered System or Appliance. Please refer to the Oracle Engineered System product documentation to understand the process for updating system components.

Oracle notifies customers about security vulnerability fixes for all its products four times a year through the Critical Patch Update (CPU) announcements program. Customers should review the CPU announcement advisories and to ensure that the latest software release updates referenced are applied to their Oracle products. Note that if a server is used in an Engineered Systems product, updates for those Engineered Systems servers will be specifically published a part of the updates for that a specific Engineered Systems product (i.e., you need not look at specific updates for individual software components included in your Engineered System). At a minimum, customers should always deploy the security updates announced in the CPU. For more information about the Oracle CPU announcements program, go to <http://www.oracle.com/technetwork/topics/security/alerts-086861.html>.

## Security Configuration Information

### Default Accounts and Passwords

This section describes the default accounts and passwords associated with this device:

#### ORACLE ILOM DEFAULT ACCOUNTS AND PASSWORDS

---

Account Name	Account Type	Default Password	Account Description
--------------	--------------	------------------	---------------------

---

root	Administrator	changeme	This is the sole default account that is delivered and enabled with this product. This account is used to perform initial configuration as well as to permit the creation of additional, non-shared administrative accounts.
------	---------------	----------	--

To list the accounts currently configured on the system, log into the Oracle ILOM and run the following command:

```
-> show /SP/users
```

To set the password for the root account, use the following commands:

```
-> set /SP/users/root password=<value>
```

Oracle ILOM has the ability to define password complexity and history by setting various parameters. One can specify the minimum password length (up to 16 characters), number of uppercase letters, lowercase letters, numbers, and symbols required. One can also enable password history. Enabling password history prevents users from using the last five previous passwords.

To view the currently configured password policy, log into the Oracle ILOM and run the following command:

```
-> show /SP/preferences/password_policy
```

```
/SP/preferences/password_policy
```

Targets:

Properties:

```
policy = 8.
min_length = 8
uppercase = no restrictions
lowercase = no restrictions
numbers = no restrictions
symbols = no restrictions
history = no restrictions
```

By default the password policy is set to a minimum length of 8 characters and no restrictions on complexity or history. For greater security, set the password policy to have a minimum length of 15 characters, and require at least one uppercase alphabetic character, one lowercase alphabetic character, one numeric character, and one special character, and enable password history. Use the following command to configure the password policy:

```
-> set /SP/preferences/password_policy policy=15.ulnsh
```

Note that when changing the password policy, all user accounts will be deleted and the factory default users will be restored. A confirmation prompt will be displayed prior to applying the new password policy. After changing the password policy from the default to a more complex one, the initial login of the root user will initiate a password change for the root user in order to enforce the new password policy for the root user.

For more information on Oracle ILOM account and password policy management see:

- » Oracle ILOM Administrator's Guide for Configuration and Maintenance (Version 3.2.x), [https://docs.oracle.com/cd/E37444\\_01/pdf/E37446.pdf](https://docs.oracle.com/cd/E37444_01/pdf/E37446.pdf)

Always review the correct version of the product security guide as the security features, capabilities and configuration options will often vary based upon product version.

## Default Exposed Network Services

This section describes the default network services that are exposed by this device:

### ORACLE ILOM DEFAULT EXPOSED NETWORK SERVICES

Service Name	Protocol	Port	Service Description
SSH	TCP	22	This port is used by the integrated Secure Shell service to enable administrative access to the Oracle ILOM using a command-line interface.
HTTP (BUI)	TCP	80	This port is used by the integrated HTTP service to enable administrative access to the Oracle ILOM using a browser interface. While TCP/80 is typically used for clear-text access, by default the Oracle ILOM will automatically redirect incoming requests to the secure version of this service running on TCP/443.
NTP	UDP	123	This port is used by the integrated Network Time Protocol (NTP) (client only) service used to synchronize the local system clock to one or more external time sources.
SNMP Agent	UDP	161	This port is used by the integrated SNMP service to provide a management interface to monitor the health of the Oracle ILOM.
HTTPS (BUI)	TCP	443	This port is used by the integrated HTTPS service to enable administrative access to the Oracle ILOM over an encrypted channel using a browser interface.  Newer systems also use this port for Remote KVMS for the Oracle ILOM Remote Console Plus service.
IPMI	TCP	623	This port is used by the integrated Intelligent Platform Management Interface (IPMI) service to provide a computer interface for various monitoring and management functions. This service is used by Oracle Enterprise Manager Ops Center to collect hardware inventory data, field replaceable unit descriptions, hardware sensor information, and hardware component status information. If Ops Center or other IPMI based management software is not in use, it should be disabled.
Remote KVMS for Oracle ILOM Remote Console	TCP	5120 5121 5123 5555 5556 7578 7579	Collectively, the Remote KVMS ports provide a set of protocols that provide remote keyboard, video, mouse and storage capabilities that can be used with the Oracle Integrated Lights Out Manager.  These ports are only exposed on older hardware. Newer systems do not expose these ports and instead use port 443 for the Remote KVMS for the Oracle ILOM Remote Console Plus service.
ServiceTag	TCP	6481	This port is used by the Oracle ServiceTag service. This is an Oracle discovery protocol used to identify servers and facilitate service requests. This service is used by products such as Oracle Enterprise Manager Ops Center to discover Oracle ILOM software and to integrate with other Oracle automatic service solutions.
Single Sign On	TCP	11626	This port is used by the integrated Sign Sign On feature that reduces the number of times a user has to enter a username and password. Disabling this service will prevent launching KVMS without having to re-enter a password.

For additional information on these services, refer to the Oracle ILOM Security Guide referenced above.

## Security Configuration Hardening

### Enable FIPS 140 Compliant Operation

The use of FIPS 140 validated cryptography is required for U.S. Federal Government customers. By default, the Oracle Integrated Lights Out Manager does not operate using FIPS 140 validated cryptography. That said, the use of FIPS 140 validated cryptography is configurable and can be enabled if required. FIPS 140 support is included in ILOM versions 3.4.x and later.

To determine if the Oracle ILOM is configured for FIPS 140 compliant operation, use the command:

```
-> show /SP/services/fips state status
```

```
/SP/services/fips
Properties:
  state = enabled
  status = enabled
```

---

*Note that FIPS 140 compliant mode in Oracle ILOM is represented by a `state` and `status` property. The `state` property represents the configured mode in Oracle ILOM and the `status` property represents the operational mode in Oracle ILOM. When the FIPS `state` property is changed, the change does not affect the operational mode (FIPS `status` property) until the next Oracle ILOM reboot or service processor reset.*

*Performing a service processor `reset` will result in the loss of all user-configured settings. For this reason, it is strongly recommended that FIPS 140 compliant operation be enabled before any additional site-specific changes are made to the Oracle ILOM. For systems where site-specific configuration changes have been made, be sure to back up the Oracle ILOM configuration so that it can be restored after the Oracle ILOM has been reset otherwise those configuration changes will be lost.*

---

To enable FIPS 140 compliant operation, use the command:

```
-> set /SP/services/fips state=enabled
```

Once configured, the Oracle ILOM service processor must be restarted for this change to take effect. To restart the Oracle ILOM service processor, use the command:

```
-> reset /SP
```

Finally, some Oracle ILOM features and capabilities are not available when configured for FIPS 140 compliant operation. A list of those features is covered in the Oracle ILOM Security Guide in the section titled "Un-Supported Features When FIPS Mode Is Enabled."


### Disable Unnecessary Services

It is recommended that customers disable any services that are not required to support the operational and management requirements of the platform. By default, the Oracle Integrated Lights Out Manager employs a network "secure by default" configuration whereby non-essential services are already disabled by default. That said, based upon customer security policies and requirements, it may be necessary to disable additional services.

To determine the list of services supported by the Oracle ILOM, use the command:

```
-> show /SP/services
```





To determine if a given service is enabled, use the command, substituting the parameter <servicename> with the name of a service returned using the previous command:

```
-> show /SP/services/<servicename> servicestate
```

While the majority of services recognize and use the `servicestate` parameter to record whether the service is enabled or disabled, there are a few services such as `servicetag`, `ssh` and `sso` that use a parameter called `state`. Regardless of the actual parameter used, a service is enabled if the service state parameter returns a value of enabled as in the following examples:

```
-> show /SP/services/https servicestate
```

```
/SP/services/https
Properties:
    servicestate = enabled
```

```
-> show /SP/services/ssh state
```

```
/SP/services/ssh
Properties:
    state = enabled
```

To disable a service that is no longer required, set the service state to disabled using a command such as:

```
-> set /SP/services/http servicestate=disabled
```


As noted above, the Oracle ILOM is delivered in a network secure by default state where non-essential services are disabled by default. That said, depending upon the tools and methods used, the following additional services may be disabled if they are not required or used:

- » Browser Administrative Interface (HTTP, HTTPS)
  - > **set /SP/services/http servicestate=disabled**
  - > **set /SP/services/http securerredirect=disabled**
  - > **set /SP/services/https servicestate=disabled**
- » Keyboard, Video, Mouse Service (KVMS)
  - > **set /SP/services/kvms servicestate=disabled**
- » Single-Sign On Services (SSO)
  - > **set /SP/services/sso state=disabled**
- » SNMP
  - > **set /SP/services/snmp servicestate=disabled**
- » IPMI
  - > **set /SP/services/ipmi servicestate=disabled**

Note that the SNMP and IPMI services are used by Oracle Enterprise Manager Ops Center and other system management software. Disabling these service will prevent Ops Center from being able to manage these devices.

On Oracle Super Cluster M7 compute nodes additional services are enabled/disabled on a per PDomain basis. These services can be accessed via `/Servers/PDomains/PDomain_X/SP/services` (where X is an integer representing a PDomain on the system.) For example: `/Servers/PDomains/PDomain_0/SP/services` will show the services for PDomain\_0 ILOM.

- » To disable KVMS service for PDomain\_0 on Super Cluster M7
  - > **set /Servers/PDomains/PDomain\_0/SP/services/kvms state=disabled**



» To disable SSO service for PDomain\_0 on Super Cluster M7  
-> **set /Servers/PDomains/PDomain\_0/SP/services/sso state=disabled**

#### Check that HTTP Redirection to HTTPS is Enabled

By default, the Oracle ILOM is configured to redirect incoming HTTP requests to the HTTPS service to ensure that all of the browser-based communications are encrypted between the Oracle ILOM and the administrator. To verify that secure redirection is enabled, use the command:

-> **show /SP/services/http securerredirect**

```
/SP/services/https
Properties:
    securerredirect = enabled
```

If the default has been changed, secure redirection can be enabled using the command:

-> **set /SP/services/http securerredirect=enabled**

Note that if both http and https services are disabled, enabling **securerredirect** will enable the https service. If you wish to keep both the http and the https services disabled you must disable **securerredirect** first then disable both http and https services.

#### Check that SSLv2 Protocol for HTTPS is Disabled

ILOM version 3.2.6 provides an improved secure-by-default configuration by completely eliminating support for SSLv2. However, older versions of ILOM provide support for SSLv2 and must be secured.

By default, the SSLv2 protocol is disabled for the HTTPS service on ILOM versions that support it. Oracle strongly recommends that customers do not change this default behavior. To determine if the SSLv2 protocol is disabled for the HTTP service, use the command:

-> **show /SP/services/https sslv2**

```
/SP/services/https
Properties:
    sslv2 = disabled
```


If the default has been changed, the SSLv2 protocol can be disabled using the command:

-> **set /SP/services/https sslv2=disabled**

#### Check that SSLv3 Protocol for HTTPS is Disabled

ILOM version 3.2.6 provides an improved secure-by-default configuration by completely eliminating support for SSLv3. However, older versions of ILOM provide support for SSLv3 and must be secured.

By default, the SSLv3 protocol is enabled for the HTTPS service on ILOM versions that support it. Oracle strongly recommends that customers disable the SSLv3 protocol. To determine if the SSLv3 protocol is disabled for the HTTP service, use the command:



```
-> show /SP/services/https sslv3
```

```
/SP/services/https
Properties:
    sslv3 = enabled
```

It is strongly recommended that SSLv3 be disabled. To disable the SSLv3 protocol, use the command:

```
-> set /SP/services/https sslv3=disabled
```

### Check that Unapproved TLS Protocols for HTTPS are Disabled

By default, the TLSv1.0 protocol is disabled while TLSv1.1 and TLSv1.2 protocols are enabled for the HTTPS service. Customers may disable one or more TLS protocol versions that do not comply with their security policy. Oracle recommends that organizations use TLSv1.2 unless support for older versions of the TLS protocol is required. To determine the list of TLS protocol versions that are enabled for the HTTPS service, use the command:

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
```

```
/SP/services/https
Properties:
    tlsv1 = disabled
    tlsv1_1 = enabled
    tlsv1_2 = enabled
```

In case the use of TLSv1.0 has been changed from the default, it can be disabled using the command:

```
-> set /SP/services/https tlsv1=disabled
```

To disable TLSv1.1, use the command:

```
-> set /SP/services/https tlsv1_1=disabled
```

### Check that SSL/TLS Weak and Medium Strength Ciphers for HTTPS are Disabled

ILOM version 3.2.6 has provides an improved secure-by-default configuration by completely eliminating support for weak and medium strength ciphers. However, older versions of ILOM provide support for SSL including support for weak and medium strength ciphers for the HTTPS service.

By default, Oracle ILOM disables the use of weak and medium strength ciphers for the HTTPS service on ILOM versions that support it. To determine if weak and medium strength ciphers are disabled, use the command:

```
-> show /SP/services/https weak_ciphers
```

```
/SP/services/https
Properties:
    weak_ciphers = disabled
```

If the default has been changed, the use of weak and medium strength ciphers can be disabled using the command:

```
-> set /SP/services/https weak_ciphers=disabled
```

## Check that Unapproved SNMP Protocols are Disabled

By default, only the SNMPv3 protocol is enabled for the SNMP service that is used to monitor and manage the Oracle ILOM. Customers should ensure that older versions of the SNMP protocol remain disabled unless required. To determine the status of each of the SNMP protocols, use the command:

```
-> show /SP/services/snmp v1 v2c v3
```

```
/SP/services/snmp
Properties:
  v1 = disabled
  v2c = disabled
  v3 = enabled
```

To disable SNMPv1, use the command:

```
-> set /SP/services/snmp v1=disabled
```

To disable SNMPv2c, use the command:

```
-> set /SP/services/snmp v2c=disabled
```

---

*Some Oracle and third-party products are limited in their support for newer SNMP protocol versions. Refer to the product documentation associated with those components to confirm their support for specific SNMP protocol versions. Ensure that Oracle ILOM is configured to support any protocol versions required by those components.*

*Version 3 of the SNMP protocol introduced support for the User-based Security Model (USM). This functionality replaces the traditional SNMP community strings with actual user accounts that can be configured with specific permissions, authentication and privacy protocols, as well as passwords. By default, the Oracle ILOM does not include any USM accounts. Customers are encouraged to configure SNMPv3 USM accounts based upon their own deployment, management and monitoring requirements.*

---

## Configure SNMP Community Strings

---

*This item is only applicable if SNMP v1 or SNMPv2c are enabled and configured for use. As a reminder, in order for SNMP to operate correctly a client and server must agree on the community string that will be used to authenticate access. Therefore, when changing SNMP community strings, be sure that the new string is configured on both the Oracle ILOM as well as any components that will attempt to connect with Oracle ILOM using the SNMP protocol.*


---

Given that SNMP is often used to monitor the health of the device, it is important that the default SNMP community strings used by the device be replaced with customer-defined values.

To create a new SNMP community string, use the command:

```
-> create /SP/services/snmp/communities/<string> permission=<access>
```

In the above example, the value of <string> should be replaced with a customer-defined value that is compliant with DoD requirements regarding the composition of SNMP community strings. Similarly, the value of the <access> should be replaced with either `ro` or `rw` depending upon whether read-only or read-write access is intended. Once new community strings are created, the default community strings should be removed.



To remove the default SNMP community strings, use the commands:

```
-> delete /SP/services/snmp/communities/public
-> delete /SP/services/snmp/communities/private
```

To verify the SNMP community strings that are configured, use the command:

```
-> show /SP/services/snmp/communities
```

On Oracle Super Cluster M7 compute nodes, some PDomains may also support the SNMP service in addition to the top level **/SP/services/snmp**. To check if this service exists in PDomain\_1 for example:

```
-> show /Servers/PDomains/PDomain_1/SP/services
```

```
/Servers/PDomains/PDomain_1/SP/services
Targets:
    kvms
    snmp
    sso
```

In the above example, the snmp service exists in PDomain\_1 and will need to be appropriately secured.

## Replace Default Self-Signed Certificates

The Oracle ILOM leverages self-signed certificates to enable the "out of the box" use of the TLS (and SSL for ILOM versions older than 3.2.6) protocols. Whenever possible, self-signed certificates should be replaced with certificates that are approved for use in the customer's environment and signed by a recognized certificate authority. To determine if the Oracle ILOM is using its default self-signed certificate, use the command:

```
-> show /SP/services/https/ssl cert_status
```

```
/SP/services/https/ssl
Properties:
    cert_status = Using Default (No custom certificate or private key loaded)
```

To install a customer-provided certificate, use the following commands:

```
-> set /SP/services/https/ssl/custom_cert load_uri=<URI_method>
-> set /SP/services/https/ssl/custom_key load_uri=<URI_method>
```


The Oracle ILOM supports a variety of methods that can be used to access the digital certificate and private key including HTTPS, HTTP, SCP, FTP, TFTP as well as pasting the information directly into a web browser interface. For more information, see the Oracle ILOM Configuration and Maintenance Guide.

## Configure Administrative Interface Inactivity Timeout (Browser)

The Oracle ILOM supports the ability to disconnect and log out administrative sessions that have been inactive for more than some pre-defined number of minutes. By default, the browser interface will timeout a session after 15 minutes.

To check the inactivity timeout parameter associated with the HTTPS service, use the command:

```
-> show /SP/services/https sessiontimeout
```



```
/SP/services/https
Properties:
    sessiontimeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

```
-> set /SP/services/https sessiontimeout=<n>
```

Similarly, to check the inactivity timeout parameter associated with the HTTP service, use the command:

```
-> show /SP/services/http sessiontimeout
```

```
/SP/services/http
Properties:
    sessiontimeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:

```
-> set /SP/services/http sessiontimeout=<n>
```

---

*The session timeout parameters associated with the HTTPS and HTTP services are set and managed independently. Be sure to set the `sessiontimeout` parameter associated each service to the customer-defined value as needed.*

---

## Configure Administrative Interface Inactivity Timeout (CLI)

The Oracle ILOM supports the ability to disconnect and log out administrative sessions that have been inactive for more than some pre-defined number of minutes. By default, the Secure Shell command line interface (CLI) has no specified timeout value, and consequently, administrative users accessing this service will remain logged in indefinitely. Oracle recommends that organizations set this parameter to match the value associated with the browser-user interface. This could be 15 minutes or some other customer-defined value.

To check the inactivity timeout parameter associated with the command line interface, use the command:

```
-> show /SP/cli timeout
```

```
/SP/cli
Properties:
    timeout = 15
```

To set the inactivity timeout parameter to a customer-defined value (<n> in minutes), use the command:


```
-> set /SP/cli timeout=<n>
```

For example, to set the inactivity timeout parameter to 15 minutes, use the command:

```
-> set /SP/cli timeout=15
```

## Configure Login Warning Banners

The Oracle ILOM supports the ability to display customer-specific messages both before and after an administrator has connected to the device. The Oracle ILOM connect message is displayed prior to authentication, whereas the login message is displayed after authentication. Optionally, a customer can configure the Oracle ILOM to require



acceptance of the login message prior to being granted access to Oracle ILOM functions. Both the connect and login messages as well as the optional acceptance requirement are implemented by both the browser and command line access interfaces.

To determine if connect and login messages are configured, use the command:

```
-> show /SP/preferences/banner connect_message login_message
```

```
/SP/preferences/banner
Properties:
  connect_message = (none)
  login_message = (none)
```

To set a connect or login message, use commands similar to the following:

```
-> set /SP/preferences/banner/connect message="Authorized Use Only"
-> set /SP/preferences/banner/login message="Authorized Use Only"
```

Once a login message has been configured, to determine if login message acceptance is enabled, use the command:

```
-> show /SP/preferences/banner/login message_acceptance
```

```
/SP/preferences/banner
Properties:
  login_message_acceptance = disabled
```

To enforce acceptance of the login message, use the command:

```
-> set /SP/preferences/banner/login message_acceptance=enabled
```

---

*Warning: Requiring login message acceptance may inhibit the correct operation of automated management processes that use Secure Shell as they may not be able or configured to respond to the acceptance request. As a result, such connections may hang or time out as the Oracle ILOM will not permit use of the command line interface until the message acceptance requirement has been satisfied. Enterprise Manager Operations Center is one such product that may use Secure Shell to manage the ILOM of a system.*

---

## Management Network Recommendations

In addition to the above security hardening procedures, the Oracle Integrated Lights Out Manager should be deployed on a dedicated, isolated management network. This will help to shield the Oracle Integrated Lights Out Manager from unauthorized or unintended network traffic. Access to this management network should be strictly controlled with access granted only to those administrators, services or devices requiring this level of access.

## Additional Information

For more information describing the features and capabilities of the Oracle Integrated Lights Out Manager as well as detailed technical instructions for the installation, configuration and management of this product, refer to the Oracle product documentation at:

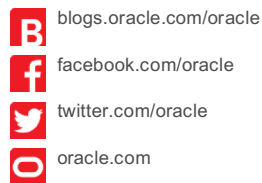


» Oracle Integrated Lights Out Manager (ILOM) 3.2 Product Documentation  
[http://docs.oracle.com/cd/E37444\\_01/](http://docs.oracle.com/cd/E37444_01/)





CONNECT WITH US



**Oracle Corporation, World Headquarters**  
500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200

**Hardware and Software, Engineered to Work Together**

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0816

Oracle Integrated Lights Out Manager Security Configuration Supplement for the United States Department of Defense  
August 2016

